


Department of the Army
First Region (ROTC)
United States Army Cadet Command
Fort Bragg, North Carolina 28310-5000

FRMOI 380-2
22 February 2002

Security

INFORMATION SYSTEMS SECURITY - USERS GUIDE

FOR THE COMMANDER:



KERRY R. PARKER
COL, AD
Chief of Staff

PROPOSER: The proposer of this publication is Information Management Division, Headquarters, First Region (ROTC), US Army Cadet Command. Comments should be sent directly to Headquarters, First Region (ROTC), ATTN: ATOA-IM, Fort Bragg, North Carolina 28310-5000.

SUPERSESSON: This FRMOI supersedes FRMOI 380-2, 24 Nov 00.

APPENDIX A: References (page 12)
B: Abbreviations (page 13)
C: Terms (page 14)

DISTRIBUTION: A; D; J; S
Distribution codes used are explained in FRMOI 25-1.

This document is available on the First Region (ROTC) Web site at:
www.rotc1.bragg.army.mil

INTRODUCTION

Computers Are Here!

From complex supercomputers to simple word processors and even laptop microcomputers, automated information systems now affect virtually every aspect of the work done in Department

of the Army activities. Computers are changing the way we do business and we rely quite heavily on them.

Today's technology places the power of the computer in your hands. You, the user of the computer system, perform data processing functions which just a few years ago only trained computer specialists performed.

Such advances offer many advantages and efficiencies, but with them come certain risks. Because we depend heavily on these systems, our missions could suffer if our computer systems or the data they process are impaired in any way.

So with all of these computer systems has come a very serious question: How can we protect them and the information they process?

In answer, we have written this FRMOI to acquaint you with computer security, or as the Army calls it, information systems security.

We have three objectives with this FRMOI:

- To introduce you to information systems security concepts.
- To outline your responsibilities for information systems security efforts.
- To provide guidelines so you can make a positive contribution to our information systems security efforts.

We hope to give you a new appreciation of some of the concerns and necessary safeguards and to show that you have an important role in protecting our automated information systems.

Feel free to share this publication with others. Talk about these issues with coworkers, family, and friends. You will find that these concerns affect many parts of your life.

Once you understand the problems we face, you will see that good security practices benefit you in many ways, both on the job and in your personal life.

PHILOSOPHY

In the relatively short time we have used computers, they have revolutionized the way the Army operates. Everyone should be aware of the critical role information systems play in day-to-

day operations. Disruption or degradation of these operations could be serious, perhaps even catastrophic.

As we become increasingly dependent on computers and telecommunications to accomplish our missions, we also become increasingly vulnerable. Vulnerabilities include compromise of classified or sensitive unclassified data, fraud, human error, accident or natural disaster, misuse of government resources, and public embarrassment from unauthorized activities.

We must take prudent measures to protect automated information systems. In fact, control is as important to an effective system as speed, capacity, or function. Benefits of good security include improved decision making and operational effectiveness, preservation of our competitive position, overall cost savings, and avoidance of public embarrassment.

Security controls are also necessary for accountability purposes. They protect honest computer users from unwarranted suspicion. Without controls, all are equally suspect when something bad happens.

While security controls may sometimes be inconvenient or inefficient, they are needed to prevent even greater loss. In the long run, effective security more than pays for itself.

THE OBJECTIVE OF INFORMATION SYSTEMS SECURITY

Our goal is to provide appropriate protection for all computer systems. Note that this objective does not apply to only some systems, such as those used to process classified information. We must protect all systems.

The phrase "appropriate protection" means that we recognize the same security measures will not apply to all systems. A computer processing classified data needs different safeguards than one handling strictly unclassified data. A word processing system does not need the same protective measures as a system that processes large amounts of financial information.

We must protect these vital information systems and the data they process against a variety of threats and hazards.

Basically, we can break these down into three main areas of protection: data confidentiality, data integrity, and data availability. We will look at each of these in detail in a moment.

HOW DOES INFORMATION SYSTEMS SECURITY HELP ME?

It Can Protect What Is Rightfully Yours.

Information is a valuable asset. To understand how valuable information can be, think about your own situation. Is information a valuable asset to you?

What If?

Computers handle your bank account and credit card records. Do you want everyone to have access to that information? Do you want just anyone to be able to modify that data, to make a withdrawal from your bank account without permission, for instance? Certainly not!

If you pay into a retirement fund or a savings account, you expect to have access to your funds in the future. How will you feel if you are denied your money because someone has carelessly or maliciously destroyed computerized information about your payments? What if there is no historical or backup information?

How many times have you tried to get some service (a catalog order or an airline reservation, for example) only to be told that they could not help you because "the computer is down"? Obviously any machine can break, but what if the problem was caused by carelessness or similar preventable action? And why didn't the business have backup processing procedures?

What About Computer Crime?

Experts estimate the losses from abuses of computer systems in the United States amount to millions of dollars each year. The businesses that suffer these crimes eventually pass the costs on to you. And these are only the obvious costs. What about the less obvious damage to these businesses caused by loss of competitive position and customer confidence?

We in the government are vulnerable to many of these same damages. And in addition to such business considerations, we must guard against espionage. The cost to the Army and the nation if sensitive or classified information is compromised could be enormous.

Is Computer Crime The Only Problem?

No. Deliberate criminal acts and espionage are only part of the problem. Experience has shown that human error, accidents, and acts of nature are frequent causes of system failure.

These acts often affect the accuracy and completeness of the data stored on computers or the availability of the computer service.

The Bottom Line Is ...

Information is valuable to all of us, personally and professionally, and needs safeguarding. By practicing good security you are not just doing a good job, you are helping to create an environment that directly benefits you.

You are protecting what is yours and what you hold in trust for others.

WHAT ARE YOUR RESPONSIBILITIES?

As a computer user, your responsibility is to maintain the confidentiality and accuracy of the data you use. You must provide protection for the information, the computer equipment, and other computer resources you use.

You are also responsible for making sure that backup copies of your important information are made and stored in a safe location. Coordinate this effort with your System Administrator or First Region (ROTC) Information Management Division.

You are personally accountable for your use of Army computers.

What Kinds of Data Must I Protect?

Our most important information is classified (Top Secret, Secret, or Confidential). The value of this information is such that we must give it special protection.

But many of us don't work with classified information. Does that mean that the data we use doesn't need protection? No! Much unclassified information is sensitive in nature and needs protection.

Sensitive unclassified data includes information protected by the Privacy Act, financial and logistical data, contractual information, For Official Use Only (FOUO) information.

The categories of classified and sensitive unclassified data are generally clear-cut. If you have any questions, talk to your System Administrator.

FRMOI 380-2
22 February 2002

Even data that is not classified or sensitive often needs protection from unauthorized modification or destruction. After all, if the data is worthless, what is it doing on a computer?

The very fact that the information is important enough to collect, process, communicate, and store shows that it has a degree of value.

That Seems Pretty Clear, Doesn't It?

Your security responsibilities aren't burdensome. Your help, however, is essential. Effective information systems security requires an ongoing commitment from everyone involved in using or managing automated systems.

WHAT CAN YOU DO TO HELP INFORMATION SYSTEMS SECURITY?

You Can Do A Lot!

You play a crucial role in protecting our automated information assets. Without your help, these vital systems could be impaired and our missions could fail.

Let's take a look at specific things you can do to assist in security efforts.

Treat Information As You Would Any Valuable Asset

You wouldn't leave cash or other valuables unprotected. You should take the same care to protect your information assets.

You can do this by safeguarding data confidentiality, data integrity, and data availability.

Data Confidentiality

This means protecting information from those who have no valid need for it. This is what comes to mind most quickly when someone mentions security, and there are many things you can do to help in this effort.

Exclude those who don't need access to your system. Don't leave your equipment unattended when you have signed on, even for just a few minutes. If you do, it becomes an invitation for anyone to use-or-abuse-it. Always log off or otherwise inactivate your system

when you are away from it. Remember, your system is to be used only by authorized personnel and only for official purposes.

Make certain no one can impersonate you. If your computer requires a user identification, a USERID or password guard them.

Your USERID identifies you specifically to the system. Your password is proof to the system that you are really who you claim.

If someone else uses your USERID or password, the system thinks that person is you. Whatever they do on the system will now be considered to be your doing and may be your fault.

If your system allows you to choose your own password, make it at least eight characters in length. Include at least one CAPITAL letter, one small letter and one number. Don't make it something obvious (such as your name or initials or that of your spouse or children or pet, social security number, address, hobbies, and so forth) or trivial (sequential numbers or letters, for example). In other words, don't use anything that can be easily guessed.

Passwords are only as effective as you make them. Make sure yours is a good one, don't share it with anyone, and change it often (immediately, if you think it is compromised). Protecting your password is a way of protecting yourself and your valuable work.

Protect telephone numbers that connect to computer systems. Never post such information or share it with others. If someone has a valid need for that information, they can get it through proper channels.

Prevent access to data to which others have no valid need. Delete files when they are no longer needed.

Practice good physical security. Lock desk drawers and, where possible, office doors. Safeguard tapes, diskettes, and other important materials by storing them inside a locked desk, file cabinet, or safe.

Dispose of classified and sensitive waste (including printouts, ribbons, diskettes, and tapes) according to approved procedures. If you are not sure of the proper procedures, check with your System Administrator.

Data Integrity

This refers to the accuracy, completeness, and timeliness of the information we process on our computers. We input vast quantities of data into our systems and then manipulate it or extract portions of it to get the specific information we need.

The final result is that some decision is made on that information. If the information is incomplete or incorrect, poor decisions will follow.

Screen input data for errors and omissions. In some cases it may even be worthwhile to have a second person compare input documents with the data keyed into the input file.

Test your system. Make sure it does what it should be doing.

Insist on and use security controls such as audit trails, reasonableness checks, and protection of key data files.

If your system operates in an abnormal or incorrect manner, tell your supervisor or System Administrator.

Remember, a computer is just a machine that does what it is told to do. It doesn't know if what you have told it to do is correct or not. Nor does it know if the information you have given it to process is correct. A computer simply processes the information the way it has been programmed to, or at least tries to. You cannot accept information as correct merely because it comes from a computer.

Data Availability

This refers to making certain we always have the capability to process the data we need. Considerations include backups for processing systems, software, and data. As a user, you have two major concerns in this regard. You must protect the primary copies of data from loss, damage, or destruction. Then you must make sure backup copies exist in case something does happen to the primary data copies.

Again, exclude those who don't need access to your system since they can accidentally or willfully cause damage or loss. Don't leave your equipment unattended when you have signed on.

Protect diskettes and tapes from spilled food and drink, cigarette smoke and ashes, excessive heat or cold, and magnetism (including the electromagnetic fields generated by radios and telephones). Diskettes in particular are fragile and should be treated with care. Never touch the exposed recording surface.

Label diskettes and tapes externally with the contents, the classification or sensitivity, and the owning organization. This will help prevent loss and errors.

Despite all protective measures, things can still go wrong. Make sure that backup copies of data and locally developed programs are made regularly, and then store them in a safe place away from the originals.

Disruptions and delays are expensive. Nobody enjoys working frantically to reenter work, do the same job twice, or fix problems while new work piles up. We can prevent most disruptions and minimize those that do occur with advance planning.

What Else Should I Do?

Don't be a software pirate. Software piracy is the illegal copying of software. Many computer programs are protected under federal copyright laws. Carefully review the licensing information that comes with software and make sure you comply with it. The penalties for illegal copying are severe - up to \$100,000 per incident or up to 5 years in prison.

Guard against computer viruses. These are hidden computer programs, often designed to damage or destroy your data or processing capabilities. Like biological viruses, they can create new copies of themselves and infect other programs. Check with your automation security representative for information on how to combat computer viruses. Use your Anti-Virus software to scan ALL disks received from other organizations prior to using on your computer.

And Last of All ...

Make a final end-of-day check to be sure that everything has been properly secured.

SECURITY MANAGEMENT

Since we rely on information systems for many jobs, we need a standard way of dealing with their security.

FRMOI 380-2
22 February 2002

AR 380-19 is the primary guide for automation security in the Army and is where you can find detailed information and specific requirements.

Establish guidelines and procedures, ensure implementation of regulations, and coordinate automation security efforts with the First Region (ROTC) Information Management Division, the focal point for these matters.

First Region (ROTC) brigades and battalions are required to have an Information Systems Security Officer (ISSO). This person is the focal point for information systems security. The ISSO is the person to turn to with questions or suggestions about computer security.

Finally, each automated system needs a System Administrator (SA). These individuals ensure that computers are operational and secure.

Information systems security involves more than just a few designated people. It concerns everyone involved with each automated system, from the system designers, through the computer programmers and operators, to the final user (clerk, secretary, manager, and so forth) of the information available from the system.

CONCLUSION

Vital data and programs can be destroyed, sensitive information revealed, financial loss suffered, or personal privacy rights violated if we don't do our part in protecting automated systems. We must act, before a serious loss or a crisis from which recovery may be difficult or impossible.

Many effective information systems security practices are just good sense and good management. They are certainly not, as they have sometimes been called, time-wasters or unproductive. In truth, good security is simply enlightened self-interest.

Effective information systems security must go far beyond the measures outlined in this FRMOI. Without your constant awareness and help, the most complex and expensive technical safeguards will be for nothing. You are the key to information security.

Take a few minutes right now to think about your system and what you can do to protect it. After all, practicing good security benefits us all.

SUMMARY

- Guard information as you would any valuable asset.
- Protect USERIDs and passwords. Don't lend, borrow, or post this information.
- Control access to your computer equipment. Don't leave it unattended while it is signed on.
- Destroy sensitive output effectively, don't just throw it in the trash.
- Prevent access to data to which others have no valid need. Safeguard data, programs, procedures, and documentation. Don't give away "road maps" of your operations.
- Erase unneeded files. Simply deleting a file doesn't actually remove the information on the disk.
- Ensure that you have backup copies of essential data and programs - and that they are stored in a safe location away from the primary copies.
- Implement good physical security. Where possible, lock your computer, desk drawers, and office doors. Secure tapes, diskettes, and other important materials by storing them inside a locked desk, file cabinet, or safe. Politely challenge people who don't belong in your area and assist them in finding the right office.
- Prohibit unauthorized software on your system. Don't use pirated software. Be certain all software comes from an authorized source to avoid computer viruses.
- Report actual or suspected violations to your System Administrator.

REFERENCES

This FRMOI has discussed a number of issues pertinent to information systems security. This is an informal publication intended to raise your awareness and to serve as a quick reference guide about specific information systems security safeguards.

If you have specific questions or recommendations concerning the protection of the systems you work with, talk to your supervisor or System Administrator.

For specific Army policies and requirements, refer to the following:

- AR 380-19
- AR 25-1
- AR 25-55
- AR 340-21
- AR 380-5

In addition to this publication, FRMOI 380-3 is available to help educate commanders and managers about protection of automated systems.

ABBREVIATIONS

FOUO

For Official Use Only

ISSO

Information System Security Officer

SA

System Administrator

USERID

User Identification. A unique code identifying each computer user.

TERMS

Audit trail

A chronological record of system activities.

Applications software

Computer programs designed to perform a specific user-oriented function, such as word processing, spreadsheets, inventory, and so forth.

Data integrity

Those aspects of data quality referring to accuracy and completeness.

Remote processing

Data processing which involves terminal devices physically located away from the central processing equipment.

Sensitive unclassified information

Information which requires protection because its unauthorized loss, disclosure, modification, or destruction could damage government operations or violate legally protected personal privacy.